Ayla Networks, Inc.
SOC 3 SysTrust
2015

SOC 3 SYSTRUST FOR SERVICE ORGANIZATIONS REPORT

July 1, 2015 To December 31, 2015

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT
ON CONTROLS AT AYLA NETWORKS, INC. RELEVANT TO
SECURITY, AVAILABILITY, AND CONFIDENTIALITY

To: Ayla Networks, Inc.

We have examined Ayla Networks, Inc. (Ayla) management assertion that, during the period July 1, 2015 To December 31, 2015, Ayla maintained effective controls over the Cloud Services Platform System for the security, availability, and confidentiality principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria) to provide reasonable assurance that:

- the system was protected against unauthorized access (both physical and logical)
- the system was available for operation and use as committed or agreed
- the system protected information designated as confidential as committed or agreed

Ayla uses Amazon Web Services ("subservice organization") for cloud hosting services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description presents Ayla's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

This assertion is the responsibility of Ayla's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Ayla's controls over the security, availability, and confidentiality of the Cloud Services Platform System, (2) testing and evaluating the operating effectiveness of the controls, (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

The criteria for the security, availability, and confidentiality principles include criterion that cannot be achieved without the implementation of controls by the subservice organization. In addition, the applicable trust services criteria require the implementation of certain complementary user-entity controls. As a result the controls placed into operation by Ayla alone are not suitably designed to meet the criteria.

In our opinion, except for the matter described in the previous paragraph, during the period July 1, 2015 To December 31, 2015, Ayla's management assertion referred to above is fairly stated, in all material respects, based on the AICPA and CICA applicable trust services criteria.

The SOC logo for Service Organizations on Ayla's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

A-LIGN

January 20, 2016
Tampa, Florida

SECTION 2

MANAGEMENT OF AYLA NETWORKS, INC.'S ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD JULY 1, 2015 TO DECEMBER 31, 2015

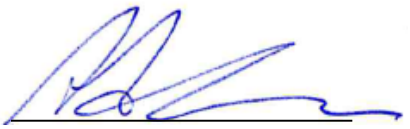
Management of Ayla Networks, Inc.'s Assertion Regarding Its System Throughout the Period July 1, 2015 to December 31, 2015

January 20, 2016

During the period July 1, 2015 To December 31, 2015, Ayla Networks, Inc. (Ayla) maintained effective controls over the Cloud Services Platform System for the security, availability, and confidentiality principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria) to provide reasonable assurance that:

- the system was protected against unauthorized access (both physical and logical)
- the system was available for operation and use as committed or agreed
- the system protected information designated as confidential as committed or agreed

Our attached System Description of the Cloud Services Platform System summarizes those aspects of this system covered by our assertion.



Adrian Caceres
VP of Engineering
Ayla Networks, Inc.

SECTION 3

DESCRIPTION OF AYLA NETWORKS, INC.'S SYSTEM THROUGHOUT THE PERIOD JULY 1, 2015 TO DECEMBER 31, 2015

OVERVIEW OF OPERATIONS

Company Background

Founded in 2010, Ayla Networks, Inc. (Ayla) provides the Agile Internet of Things (IoT) platform, accelerating development, support, and ongoing enhancements of connected products for the IoT. Ayla's end-to-end platform runs across devices, cloud, and applications to create secure connectivity, data analytics, and feature-rich customer experiences. Delivered as a cloud platform-as-a-service (PaaS), Ayla's Agile IoT platform provides the flexibility and modularity to enable rapid changes to practically any type of device, cloud, or application environment.

Description of Services Provided

Ayla Networks, Inc. helps its customers create connected devices for the IoT. The company works with Wi-Fi "Module" vendors to create module packages pre-loaded to connect to the Ayla Could Service. Ayla helps its customers to:

- Connect their products to the Internet using these standardized Wi-Fi modules
- Operate/monitor their devices that have been sold to their end users
- Develop smart phone applications for their end users to monitor/control devices via the Ayla Cloud Service Platform

Typical products are devices like thermostats, garage door openers, etc. which an end user, typically a home owner, controls via a smart phone applications, after having connected the device to their home wireless network.

Infrastructure

Ayla's Cloud Service Platform system is implemented on Amazon AWS, in an AWS VPC, and makes use of numerous AWS services.

Software

Ayla's Cloud Service Platform system includes both Ayla-authored and 3rd party software running on the AWS EC2 instances.

People

Ayla Networks' staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Cloud Services Development team - responsible for delivering a responsive system that fully complies with the functional specification
- Quality Assurance team - a sub-set of the Cloud Services Dev Team - verifies that the system complies with the functional specification through functional testing procedures
- DevOps team - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Success Team - serves customers by providing product and service information that includes resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Procedures

Informal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Ayla policies and procedures that define how services should be delivered.

Physical Security

The company has two main facilities. The home office is in Sunnyvale, California.

Logical Access

Ayla's IT infrastructure is largely outsourced. All users of the systems are to be identified and authenticated prior to the use of any system resources. As people are hired/terminated the various administrators adjust who can access the outsourced sites.

All resources are managed in the asset inventory system, including those that are outsourced, and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Customer employees' access Ayla's IoT enablement platform services through the internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources.

Upon hire, Ayla's employees are assigned to a position in the HR management system. They are issued a user name under Ayla's Domain. This user name and a password are created by the user, and are used to access numerous applications. Individual departments often have outsourced applications.

At the point in time when an employee is terminated, HR removes them from the HR systems which automatically ends their payroll, and benefits access. IT terminates the employee's generic accounts. The individual's manager is asked to terminate any group-specific access.

Computer Operations - Backups

Customer data is backed up automatically and, essentially, continuously.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network.

Ayla monitors the capacity utilization of its computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Ayla evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data storage
- Computer utilization

Ayla has implemented a patch management process to ensure contracted customer systems are patched in accordance with vendor recommended operating system patches. Ayla system owners review proposed operating system patches to determine whether the patches are applied. Ayla is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Ayla staff validate that all patches have been installed, and if applicable, that reboots have been completed.

Change Control

Ayla maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are documented and maintained. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the internet and deny any type of network connection that is not explicitly authorized.

Penetration testing is conducted to measure the security posture of Ayla's customer-facing environment. The third party vendor uses an accepted industry standard penetration testing methodology specified by Ayla. The third party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by Ayla in delivering its Cloud Service Platform system. Data related to OEM accounts and end-users includes, but is not limited to:

- Name
- Email address
- Phone number
- Wireless network and location of the connected device(s)

Boundaries of the System

The scope of this report includes the Ayla Cloud Service Platform performed in the Sunnyvale, California facility.

Significant Events and Conditions

Ayla has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Cloud Service Platform system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Events and conditions include, but are not limited to:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Preparation and Delivery of Reports and Data

Ayla utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.